






Encryption and decryption method and apparatus

Patent number: CN1249096
Publication date: 2000-03-29
Inventor: SUMNER TERENCE EDWARD (US)
Applicant: MOTOROLA INC (US)
Classification:
- **international:** H04L9/32
- **europaean:** H04L9/08; H04L29/06C6B; H04L29/06C6G
Application number: CN19980802839 19980109
Priority number(s): US19970791968 19970131

Also published as:

 WO9834374 (A1)
 EP0962072 (A1)
 US6009173 (A1)
 CA2278670 (A1)
 CN1155198C (C)

Report a data error here

Abstract not available for CN1249096

Abstract of corresponding document: **US6009173**

A method for efficient encryption and decryption (100) comprises the steps of encrypting a message (104) at a sending unit which is to be sent to a receiving unit using a message key (106) and appending to the message at the sending unit the message key encrypted (108 and 109) using a receiver's public key (110). Subsequently, a sender's certificate (116) is appended at a first server (302) and extracted at a second server (310). The message key is then decrypted at the receiving unit using a receiver's private key (140) to provide a decrypted message key. Subsequently the message is decrypted using the decrypted message key (142 & 143) and authenticated by comparing a pair of digest (152 and 156).

Data supplied from the **esp@cenet** database - Worldwide

[19]中华人民共和国国家知识产权局

[51]Int. Cl⁷

HD4L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 98802839.5

[43]公开日 2000年3月29日

[11]公开号 CN 1249096A

[22]申请日 1998.1.9 [21]申请号 98802839.5

[30]优先权

[32]1997.1.31 [33]US[31]08/791,968

[86]国际申请 PCT/US98/00291 1998.1.9

[87]国际公布 WO98/34374 英 1998.8.6

[85]进入国家阶段日期 1999.7.30

[71]申请人 摩托罗拉公司

地址 美国伊利诺斯

[72]发明人 特林斯·艾德华·萨穆纳

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

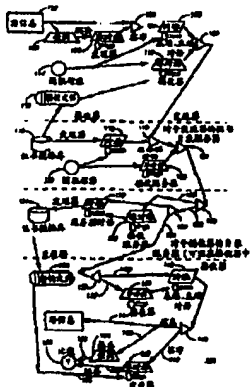
代理人 马 浩

权利要求书 3 页 说明书 10 页 附图页数 4 页

[54]发明名称 加密与解密方法及装置

[57]摘要

一种有效加密和解密的方法(100)包括以下步骤:使用信息密钥(106)在发送单元对要被发送到接收单元的信息(104)进行加密,并在发送单元使用接收器的公共密钥(110)把加密的信息密钥附加到该信息上(108和109)。然后,发送器的证书(116)在第一服务器(302)被附加并在第二服务器(310)被抽取。然后在接收单元使用接收器专用密钥(140)对信息密钥解密以便提供解密的信息密钥。然后使用解密的信息密钥(142和143)对信息解密,并通过比较一对摘要(152和156)进行鉴定。



ISSN 1008-4274

权 利 要 求 书

1.一种用于有效加密和解密的方法，包括以下步骤：

在发送单元使用信息密钥加密要发送到接收单元的信息；

在发送单元把使用接收器的公共密钥加密的信息密钥附加到信息上；

然后在第一服务器附加发送器的证书；

在第二服务器抽取发送器证书；

在接收单元使用接收器的专用密钥解密信息密钥以便提供解密的信息密钥；

然后使用解密的信息密钥解密信息。

2.根据权利要求1的有效加密和解密方法，其中加密信息的步骤还包括添加签字的步骤，通过使用单向函数产生信息的摘要并使用专用密钥加密摘要以生成加密的签署信息，专用密钥对应于嵌入发送器证书的公共密钥。

3.根据权利要求1的方法，其中的方法还包括使用服务器对话密钥加密带有服务器证书信息以提供带有证书的加密的信息的步骤，并在第二服务器使用服务器对话密钥解密带有证书的加密信息的步骤。

4.一种使用发送服务器和接收服务器从发送器向接收器有效传递带有信封的加密签署信息的方法，接收服务器使用非对称公用-专用密钥对，该方法包括以下步骤：

使用服务器到服务器对话密钥加密证书以生成加密的证书，并把加密的证书与包含以接收服务器非对称公共密钥加密的服务器到服务器对话密钥的信封连接，以便生成带有信封的加密的证书；以及

把加密的带有信封的签署信息连接到带有信封的加密的证书中。

5.根据权利要求4的方法，其中该方法还包括使用接收服务器专

用密钥解密服务器到服务器对话密钥的步骤。

6.根据权利要求5的方法,其中该方法还包括从加密的带有信封的签署信息分开证书,并进而使用服务器到服务器对话密钥解密证书的步骤。

7.根据权利要求6的方法,其中该方法还包括在接收服务器从证书抽取发送器的公共密钥的步骤。

8.根据权利要求8的方法,其中该方法还包括在接收器从加密的签署信息分开信封并解密信封以提供发送器-接收器对话密钥的步骤。

9.一种供无线通信中使用的远程证书服务器,包括:

一个用于接收加密的带有信封的无线信息的发送器服务器部分,包括:

一个用于存储加密的无线信息的存储器; 以及

一个用于以服务器到服务器对话密钥加密证书以便提供加密的证书并用于把加密的证书附加到加密的带有信封无线信息中以便提供带有信封的加密的证书和无线信息的处理器,该处理器还通过使用接收器服务器部分的非对称公共密钥来加密服务器到服务器对话密钥,以提供加密的服务器到服务器对话密钥,其中加密的服务器到服务器对话密钥被附加在带有信封的加密的证书和无线信息中。

10.根据权利要求9的远程证书服务器,其中远程证书服务器还包括接收器服务器部分,用于接收附加在加密的证书和带有信封的无线信息中的加密的服务器到服务器对话密钥,其中接收器服务器部分包括:

一个存储器,用于存储附加在加密的证书和带有信封的无线信息中的加密的服务器到服务器对话密钥; 以及

一个处理器,用于使用对应于接收器服务器部分非对称公共密钥的非对称的专用密钥,来恢复服务器到服务器对话密钥,用于把加密的证书从加密的带有信封的无线信息分开,并用于对加密的证书解密。

11. 一种使用发送服务器和接收服务器从发送器向接收器有效传送带有信封的加密签署信息的方法，接收服务器使用非对称公用-专用密钥对，该方法包括以下步骤：

从发送器向接收器发送加密的签署信息，发送器在发送服务器和接收服务器之间触发询问，看证书是否需要向接收器传送；

如果没有先前的证书接收或如果证书过期或发生其它方式的无效，则向接收器发送证书，否则按发送服务器和接收服务器之间的询问确定，发送所需证书的部分；以及

按接收器的需要解密证书或证书的一些部分。

12. 根据权利要求 11 的方法，其中如果发送服务器和接收服务器之间询问确定，证书需要被发送到接收器，则该方法还包括以下步骤：

使用服务器到服务器对话密钥加密证书以生成加密的证书，并把加密的证书与包含以接收服务器非对称公共密钥加密的服务器对服务器对话密钥的信封连接，以便生成带有信封的加密的证书；以及

把加密的带有信封的签署信息连接到带有信封的加密的证书中。

13. 一种使用发送服务器和接收服务器从发送器到接收器有效传送签署的信息的方法，该方法包括步骤：

从发送单元发送签署的信息以便在接收单元接收；

然后在第一服务器把发送器证书附加到签署信息上；

在第二服务器抽取发送器的证书；以及

在接收单元接收签署的信息，并在接收单元使用一组来自发送器证书的信息读取该信息。

说明书

加密与解密方法及装置

本发明涉及加密和解密；更准确地说，涉及在加密/解密方案中证书的有效附加。

广义来说，诸如寻呼这样的无线应用的有效寻呼 and 安全性具有相反的约束。一方面，寻呼使用其非实时功能去组合消息以便有效地降低无线带宽的无效使用。另一方面，诸如加密这样的安全性措施一般添加到正在通过空中传输的信息中。增加的用户数和信息的平均大小的增加(包括文本、传真、音频甚至视频信息)只是进一步对所提供的有限带宽的使用施加了约束。

在用于从发送器到接收器传送带有签字的安全信息的常规过程中，方法 10 中的步骤一般如以下参照图 1 所描绘的。首先用户在步骤 12 生成文本信息。然后，用户在步骤 14 使用单向函数(例如，安全散列函数)产生文本信息的摘要。然后通过步骤 20 使用他的签字或专用密钥对摘要进行的第一加密，用户在步骤 18 附加他的签字，并通过非对称引擎 16 使之运行，专用密钥一般对应于在可跟踪的证书 26 中可找到的公共密钥。然后在步骤 22 附加信息和数字签字。然后在步骤 27 把带有签字 24 的信息连接到可跟踪的证书 26，以便生成可鉴定的信息 28。然后使用对称引擎 30 和对话密钥 32 对可鉴定的信息 28 加密，以便提供加密的信息 40。使用接收器的非对称公共密钥 34 及非对称引擎 36 对对话密钥 32(通常是随机对称密钥)本身加密，以便生成数字信封 38。然后加密的信息 40 在步骤 42 被附加到数字信封 38 以生成带有信封的加密的信息加签字加证书 44。

参见图 2，典型的解密过程以把带有信封的加密的信息加签字加证书 44 的各成分，分开(46)为加密的信息 56 和数字信封 48 开始。数字信封 48 最好与图 1 的数字信封 38 相同。对话密钥 54(对话密钥

54 与图 1 的对话密钥 32 最好相同)由接收器使用他们的专用密钥 52(对应于接收器的专用密钥 34)恢复, 并通过非对称引擎 49 使用专用密钥 52 运行数字信封 48. 使用对话密钥 54 解密带有签字的加密信息 56. 换言之, 使用对话密钥 54 通过对称引擎 58 运行解密的信息 56, 以获得可鉴定的信息 60(这应当与图 1 的可鉴定信息 28 相同). 这样, 如以下几个步骤所见, 接收器能够确认(到合理的程度)信息发送器的身份. 然后, 可鉴定的信息被分为(62)证书 64 和分开的签署信息 68, 分别对应于图 1 的证书 26 和签署的信息 24. 签署的信息 68 本身还将被分开(70)为可读的文本信息 80 和数字签字 72, 分别对应于图 1 的信息 12 和数字签字 18. 从证书 64 抽取发送器的公共密钥 66, 然后用它把签字解密为摘要 77. 换言之, 使用发送器的公共密钥使数字签字 72 通过非对称引擎 74 以提供摘要 77, 这应当是实际摘要的拷贝. 通过相同的(散列)函数(如图 1 的步骤 14)使文本信息 80 运行, 以检索实际的摘要 79. 在步骤 76 实际的摘要 79 和摘要 77 进行比较, 以检验真实的签字. 注意, 在以上的例子中, 证书嵌入到加密的信息中, 从而大大增加了加密信息的大小.

图 1 是已知的用于发送信息的加密方法的流程图.

图 2 是已知的用于接收信息的解密方法的流程图.

图 3 是根据本发明实施例的加密方法的流程图.

图 4 是根据本发明的另一实施例的加密方法的另一流程图.

图 5 是根据本发明的证书服务器的框图.

参见图 3, 其中示出一种有效的加密和解密方法, 包括在发送单元使用信息密钥 112 加密要发送到接收单元的信息 102 的步骤. 然后, 使用接收器的公共密钥 110 在发送单元把信息密钥附加到信息上. 这一步骤最好包含通过使用单向函数 104 产生信息的摘要, 并使用发送器的专用密钥 106 加密摘要而添加签字, 以便生成签署的信息这样一些步骤, 专用密钥对应于嵌入在发送器证书(116)中的公共密钥. 然后在第一服务器附加一个发送器证书. 然后, 在第二服务器抽取发送器证书(134), 并然后在接收单元使用接收器专用密钥

140 解密信息密钥，以便提供解密的信息密钥。然后，使用解密的信息密钥解密信息。此外，该方法还包括使用发送器-接收器对话密钥 108 加密签署信息而提供加密的签署信息，并在接收器处使用另一发送器-接收器对话密钥 142 对加密的签署信息进行解密这样一些步骤。最好使用从第一服务器检索的接收器的公共密钥对发送器-接收器对话密钥进行加密，并作为信封把它连接到签署的信息。

在本发明的另一实施例中，使用发送服务器和接收服务器，从发送器向接收器有效传送带有信封的加密签署信息的方法，包括以下步骤：使用服务器对服务器对话密钥 118 加密证书以生成加密的证书，并使加密的证书与包含服务器对服务器对话密钥的信封连接，而服务器对服务器对话密钥是以接收服务器非对称公共密钥 120 加密的，以便生成加密的带有信封证书，并然后把带有信封的加密的签署信息与带有信封的加密的证书连接。该方法能够进一步包含以下步骤：使用接收服务器的专用密钥 130 解密服务器对服务器对话密钥，以及把证书从带有信封的加密的签署信息分开，并进一步使用服务器对服务器对话密钥 132 解密证书。此外，该方法能够包含在接收服务器处从证书抽取发送器公共密钥的步骤。在接收单元处，信封能够从加密的签署信息分开，其中信封被解密以提供发送器-接收器对话密钥。而且，能够使用发送器-接收器对话密钥去解密签署信息和签字。如以下进一步详细说明，能够使用发送器的公共密钥把在接收器处的签字解密为摘要，供与信息相关的签字的鉴定之用。这样，通过使信息通过单向函数分离信息并获得实际的摘要，该摘要与通过使用发送器公共密钥解密签字而找到的摘要进行比较，从而进行鉴定。

又，参见图 3，方法 100 示出在没有向接收单元传送证书的情形下，加密信息如何从发送单元发送到接收单元，这当发送单元和接收单元之间的通路是无线时是特别有用的。如前所述，在步骤 102 用户生成文本信息，并然后在步骤 104 使用单向函数(例如安全散列)产生文本信息摘要。用户在步骤 105 使用他的签字密钥通过非对称

引擎 106 加密摘要, 并把结果附加在信息上, 从而形成他的签字, 其中签字密钥一般是对应于在最好是可跟踪证书这样的证书中找到的公共密钥的专用密钥。然后在步骤 108 使用发送器-接收器对话密钥(通常是随机对称密钥)对签署的信息加密。在步骤 110 使用接收器的公共密钥对发送器-接收器对话密钥本身加密, 并在步骤 109 作为信封连接到签署的信息上。在步骤 108 和 110 最好使用随机信源 114 产生密钥。接收器公共密钥能够驻留在密钥文件 112 中, 或如果需要最好从发送器证书数据库 116 中抽取。在步骤 118 使用服务器-服务器对话密钥(通常是随机对称密钥)对可跟踪证书或发送器证书(116)加密, 并然后在步骤 119 连接到带有信封的加密的签署的信息上。这可选地是与发送器-接收器密钥相同的对话密钥, 但是需要对服务器进行确认。在步骤 120 使用接收服务器的非对称公共密钥对发送器-接收器对话密钥(通常也是随机对称密钥)自身加密, 并在步骤 121 连接到带有信封加加密证书的加密签署的信息上。在步骤 118 和 120 最好使用随机信源 122 产生密钥。

在接收端(从服务器到服务器的观点来看), 在步骤 130 通过接收服务器使用其非对称专用密钥来恢复加密的服务器到服务器对话密钥。在步骤 123 和 127 从带有信封的加密的签署信息(124 或 125)分开加密的证书(126), 并在步骤 132 使用对话密钥解密。最好从证书数据库 134 中的证书抽取发送器公共密钥, 如果必要, 通过向密钥文件 136 发送所需的信息供后来比较以作出鉴定。鉴定最好涉及允许跟踪授权签署源的可跟踪证书, 以便验证证书的持有者。嵌入在证书中的信息能够包含链接可跟踪授权层的较高授权的签字。这样, 通过检验可证明证书真实性的授权的签字而进行鉴定, 并然后把公共密钥与某些已经被鉴定的标识信息和证明归入密钥文件中。如果接收器已经具有公共密钥, 则服务器除了对接收器鉴别适当的公共密钥(发送器的)之外, 不采取任何行动。如果接收器没有任何密钥, 则服务器可能发送整个的证书或只是一部分证书(例如公共密钥), 作为发送和接收双方之间的相互认可。然后, 在步骤 137 从加

密的签署信息(139)分开信封(138), 并在步骤 142 由接收器使用发送器-接收器对话密钥对其解密。对话密钥(142)用来解密信息加签字。在步骤 143 信息从签字分开之后, 在步骤 148 使用发送器公共密钥(该密钥如果还没有得到可从密钥文件 136 获得)解密签字(146), 以提供摘要(152)。信息被分开(144 和 145)并通过单向函数 154 以便获得信息的实际摘要 156。把摘要 152 与实际摘要 156 进行比较以验证真实的签字。注意, 签字的鉴定是可选的, 但是对于金融应用是特别需要的。

如上所述, 不是通过发送嵌入在入站信息中的证书, 而是使证书或目录服务器从文件附加证书, 可降低越空业务量。一般来说, 与整个信息和签字只有几百位相比, 这些证书长度有上千位。通常证书通过加密覆盖, 以便对交易者提供某种程度的私密性。

实际上, 服务器向发送器或接收器或两者提供公共密钥(非对称密钥)证书目录服务, 与先有的方案比较这是新的结构。对称加密表现在发送单元(传信装置)和接收单元之间, 并标以“端到端对话”。这是可选的, 但如果需要交易的私密性而不只是鉴定和签字的私密性, 则很可能要使用。这一加密因为其简单和有效而很可能是对称的, 但是非对称的也可使用。

在发送器和服务器或载波之间没有示出寻址、控制和鉴定信息, 但是这些对于传信的目的是必须的。鉴定用在服务器和装置之间以保证服务器的安全, 装置是真实的信源以便能够附加真实的证书。控制将执行这样一些功能, 诸如处理和投送的优先性、安全性等级、及其它辅助功能。如果出现, 可能在清除中或通过服务器-装置加密进行寻址。由于私密性在日常事物中变得越来越多, 故甚至在使用广播媒体时寻址可能也要需要防止窥视的眼睛。

参见图 5, 供无线通信使用的远程证书服务器 300, 包括用于接收带有信封的加密无线信息的发送器服务器部分 302, 以及用于存储加密无线信息的存储器 304。发送器服务器部分还包括用于以服务器到服务器对话密钥加密证书以便提供加密证书的处理器 306。处理器

306 还把加密的证书结合到带有信封的加密的无线信息中,以便提供加密的证书和带有信封的无线信息。处理器 306 还使用接收器服务器部分的非对称公共密钥来加密服务器到服务器对话密钥,以提供加密的服务器到服务器对话密钥,其中加密的服务器到服务器对话密钥被附加到加密的证书和带有信封的无线信息中。远程证书服务器 300 还包括接收器服务器部分 310,用于接收附加到加密的证书和带有信封的无线信息中的加密的服务器到服务器对话密钥。接收器服务器部分 310 最好包括存储器 308,用于存储附加到加密的证书和带有信封的无线信息中的加密的服务器到服务器对话密钥;以及处理器 309,用于使用对应于接收器服务器部分的非对称公共密钥的非对称专用密钥来恢复服务器到服务器对话密钥,并用于从带有信封的加密的无线信息中分开加密的证书,并用于对加密的证书解密。应当注意,远程证书服务器 300 的发送器服务器部分 302 和接收器服务器部分 310 能够通过所需有线网络或无线网络硬连接或耦合在一起。

接收器公共密钥或接收单元的证书必须从服务器转移到发送器。服务器能够发送整个证书,并允许发送器鉴定嵌入的信息,或者发送器和服务器能够具有置信的相互关系,允许发送器对于图 3 中步骤 112 所示的密钥文件中的位置刚好获得证书的密钥部分。为了尽量减少后来的问题,服务器还应当通知密钥的过期或有效性,并为了尽量减少后来的业务量,发送器和服务器应当在表示证书持有者诸如标签或名字的令牌上一致。

参见图 3,如前面所指出的,末端到末端对话密钥可以是对称的。一般来说,对称密钥需要附加的同步化(例如开始向量)信息,以便正确地工作。这一点图中没有明显示出。这也适用于服务器-服务器对话密钥。证书(加任何附加的路由和中继信息)由这一对话密钥覆盖。这一密钥的同步化信息可从末端-末端对话密钥的同步化或已经在信道上的其它信息推导,以便降低开销。密钥本身可以是用于末端-末端对话的相同的密钥,但这将生成潜在的安全问题。这问题在

于, 服务器应当有充分的能力对信息进行解密。如果两个服务器对发送器和接收器两者都是置信的, 则这不构成问题。避免这一问题的及一般的解决办法应当要求服务器-服务器对话密钥相对末端-末端对话密钥是唯一的。

接收器和接收服务器能够是一个并是同一实体, 使得寿命简单。发送器证书能够与入站信息分开并被鉴定(未示出)和归档。当传信装置是这种信息的接收器时, 能够类似地降低越过空中的业务量。但是这多少更困难一些。发送器在其整体中的证书由接收器保有或就是发送器的密钥。除非必需, 发送服务器不会随意(suthomatically)发送证书, 在很多情形下这将只对证书的单一传输降低业务量。进而, 接收器和接收服务器可以与业务量的考虑限制较少的有线网络连接。当传信装置仅具有密钥时, 信息可被解密, 但丧失了可跟踪性, 除非整个的证书由传信装置保有直到被验证为止。类似地, 服务器和发送服务器能够是一个并且是同一实体, 特别是如果没有来自发送器的无线通路。

接收服务器可以是置信的或非置信的。如果是置信的, 则传信装置仅保有密钥。如果是非置信的, 则传信装置保有整个证书。对于非置信存储器上的蕴含和装置中的处理要求至少在证书鉴定时暂时有大得多的能力。一旦被验证, 则只需保持密钥及其期限。通过空中的业务量也增加, 以便允许证书向接收者的传输及他们来自最终权威结机构的鉴定的传输。服务器能够剔除不必要的证书, 而只发送以前从未发送过的那些证书。这象是发送服务器的处理或带有标签或名字的接收器证书。即使证书已经被发送过, 如果接收器没有识别出服务器使用的标签和名字, 则它也能够刷新证书或密钥。参见图 4 可以看到几个这种实施例的例子。

图 4 示出用于从发送单元向接收单元发送信息方法的另外的实施例。具体来说, 方法 200 表示加密的信息如何从发送单元向接收单元发送, 而不必在每次发送信息时向接收单元传输证书。如前所述, 用户在步骤 202 生成文本信息, 并然后在步骤 204 使用单向函

数(例如安全散列)产生文本信息的摘要。用户通过使用其签字密钥通过对称引擎 206 对摘要加密来形成它的签字,并在步骤 205 把结果附加到信息中,其中签字密钥一般是对应于在可跟踪证书中找到的公共密钥的专用密钥。然后在步骤 208 使用发送器-接收器对话密钥(或末端-末端对话密钥)(通常是随机对称密钥)加密签署的信息。在步骤 210 使用接收器公共密钥对发送器-接收器对话密钥本身加密,并在步骤 209 作为信封连接到签署的信息中。在步骤 208 和 210 最好使用随机信源 214 产生密钥。接收器公共密钥能够驻留在密钥文件 212 中,或必要时最好从发送器证书数据库 216 中抽取。

在步骤 211,发送单元能够直接向接收单元发送带有信封的签署的信息,而不需要来自服务器的任何其它东西。例如,如果以前在发送单元和接收单元之间发送过信息,则接收单元可能已经有用来鉴定信息的证书(在接收单元)。另外,接收单元为鉴定信息可能只需要来自密钥文件(231)的密钥。换言之,接收单元可能只需要来自证书的部分信息(而不是整个证书),这将有助于降低在诸如两个经常通信者,诸如销售商和经常的购买者之间看到的空中业务量。

这样在本发明的一个实施例中,信息从发送单元到接收单元的发送(211)可能需要另一通路 213,其中在步骤 223 信息与加密的可跟踪证书或带有信封的发送器的证书(216)连接。最好在步骤 218 使用服务器-服务器对话密钥(通常是随机对称密钥)加密证书 216,并然后在步骤 221 与接收服务器的公共密钥 220 连接,以便提供带有信封的加密的证书。在步骤 218 和 220 最好使用随机信源 222 产生密钥。带有信封加密的信息和带有信封加密的证书能够或者如前对图 3 所述那样通过类似的解密算法运行,或者加密的信息能够通过步骤 225 取另一路由 227 到接收单元,其中不需要来自接收服务器的任何信息或只需最小信息去解密和/或鉴定加密的信息。

在需要整个证书或证书的一部分的情形下,在步骤 229 信封与加密的证书被分开。使用接收服务器的专用密钥 224 鉴定服务器发送信息,并使用服务器-服务器对话密钥 226 解密存储在证书数据库

228 中的证书。证书或证书适当的部分(诸如密钥)能够转发给密钥文件 231, 用于后来由接收单元进行的鉴定。带有信封的签署的加密信息或是由通路 211 或是 277 发送, 在步骤 233 信封从签署加密的信息分开。在步骤 232 接收器公共密钥用来剔除信封, 并在步骤 234 末端-末端对话密钥解密签署的加密信息。在步骤 235 签署的加密信息本身再次被分开为信息和签字。信息通过散列函数 240 获得信息的实际的摘要 242。在步骤 236 使用发送器的公共密钥解密签字以获得摘要 244。然后摘要 244 与实际的摘要 242 进行比较以验证真实的签字。还要注意, 签字的鉴定是可选的, 但是特别对于金融方面的应用是需要的。

图 4 示出根据本发明的另外两个实施例。在第一种情形下, 信息不带证书地被加密并被发送到接收单元(211), 同时各服务器分开地(由发送单元触发)通信和决定证书的拷贝是否需要发送到接收单元(如所示最好以加密的形式)。然后接收服务器解密、存储、并发送接收单元所需的证书或证书的密钥。在第二种情形下, 对信息加密并然后附加到证书中。证书本身最好由服务器加密。然后加密的信息以及加密的证书被发送到接收服务器, 其中接收服务器分拆证书、对其加密、存储并把证书或密钥发送到接收单元。

在本发明的广义方面, 使用发送服务器和接收服务器从发送器向接收器有效地传输签署的信息的方法包括步骤: 从发送单元发送签署的信息供接收单元接收, 并然后把在第一服务器处的发送器的证书附加到签署的信息上。发送器的证书及甚至签署的信息可选地被加密。在第二服务器, 抽取发送器的证书, 并使用从发送器证书抽取的一组信息在接收单元接收和读取这样签署的信息。这组信息最好从名字、公共密钥、签字机构、期限日期、有效期、发放日期、控制号码、或其它适当的信息组抽取。

能够接收或连接到智能卡的个人管理单元(PMU)或用户单元在本发明权利要求书的意图之内。实际的实现能够包括带有供插入智能卡接头的 PMU, 或者带有供由电缆连接到 PMU 的智能卡用的分

开的接口单元的 PMU, 或者带有固定的或可拆卸的嵌入的智能卡的 PMU. 证书服务器可作为自包含单元(甚至包含在 PMU 内部), 或者作为传信开关内运行的软件程序(寻呼或传信终端), 或者整个作为传信系统域之外的外部开关来实现. 假设证书服务器将为充分的可兼容协议支持而提供对应的实体, 包括适当的加密方案和对最终权威机构的访问的使用以便鉴定.

应当理解, 透露的实施例仅是示例性的, 并且本发明不限于此. 业内专业人员将能够理解, 在如所附权利要求书定义的本发明的范围和精神之内能够作出各种变形和修改.

说明书附图

10

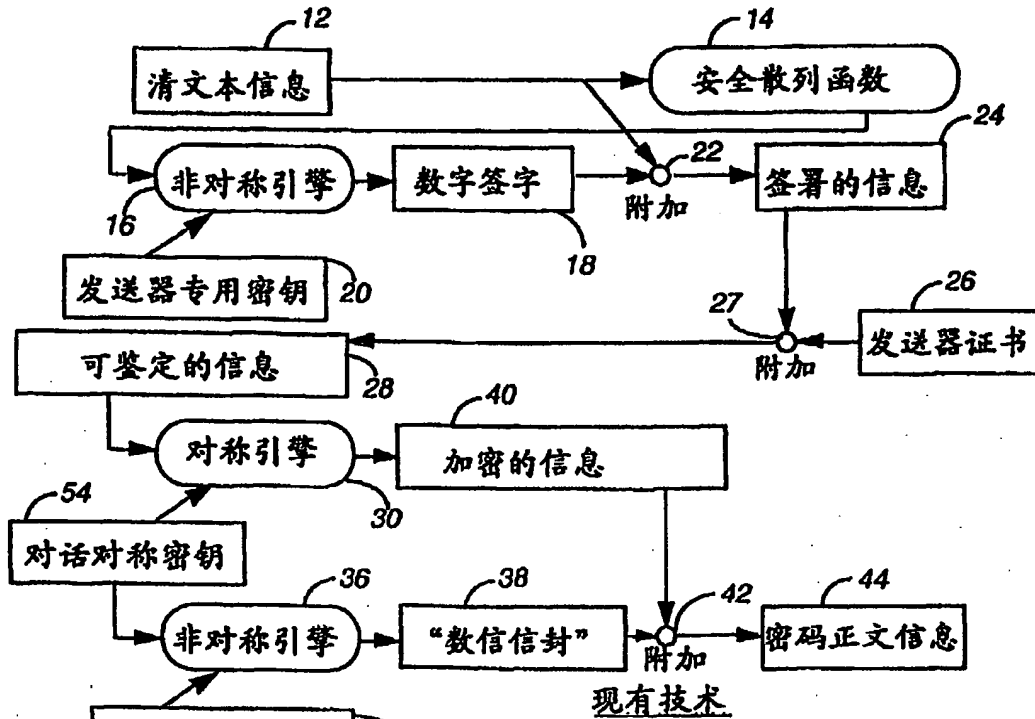


图1

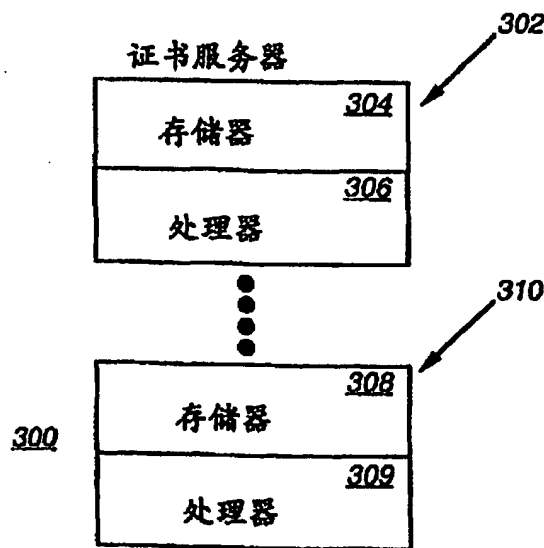
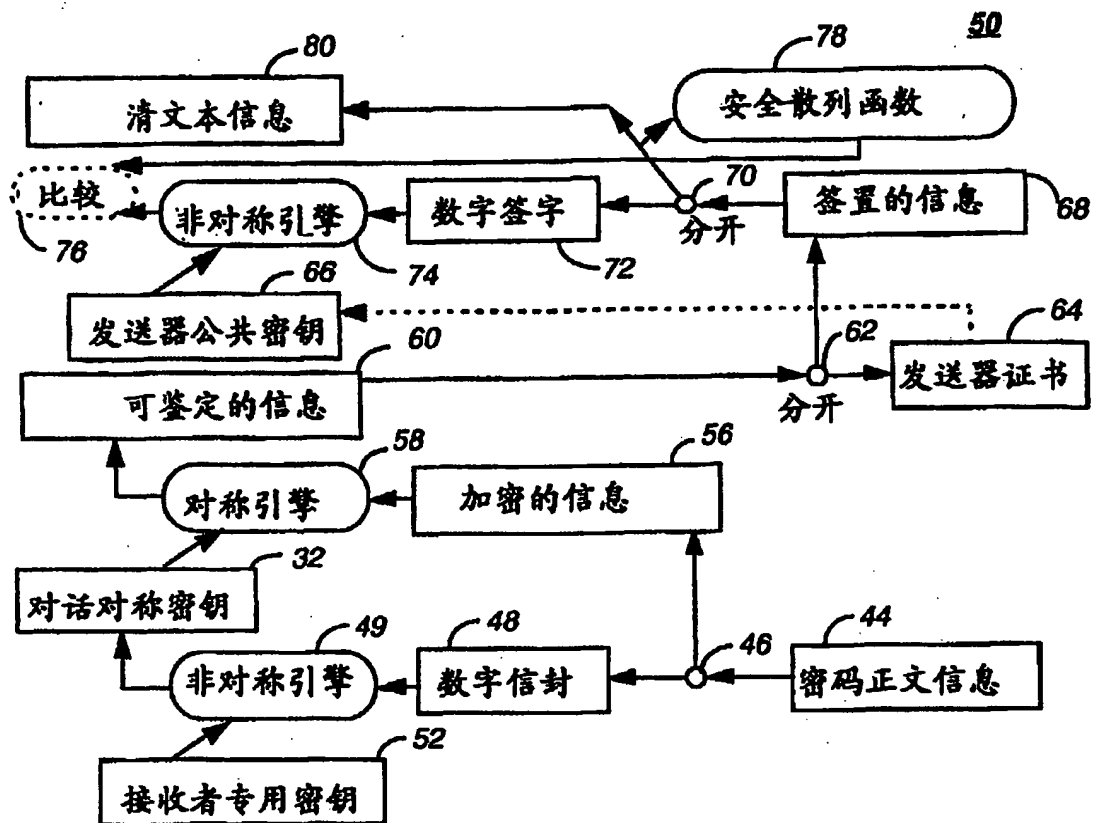


图5



现有技术

图 2

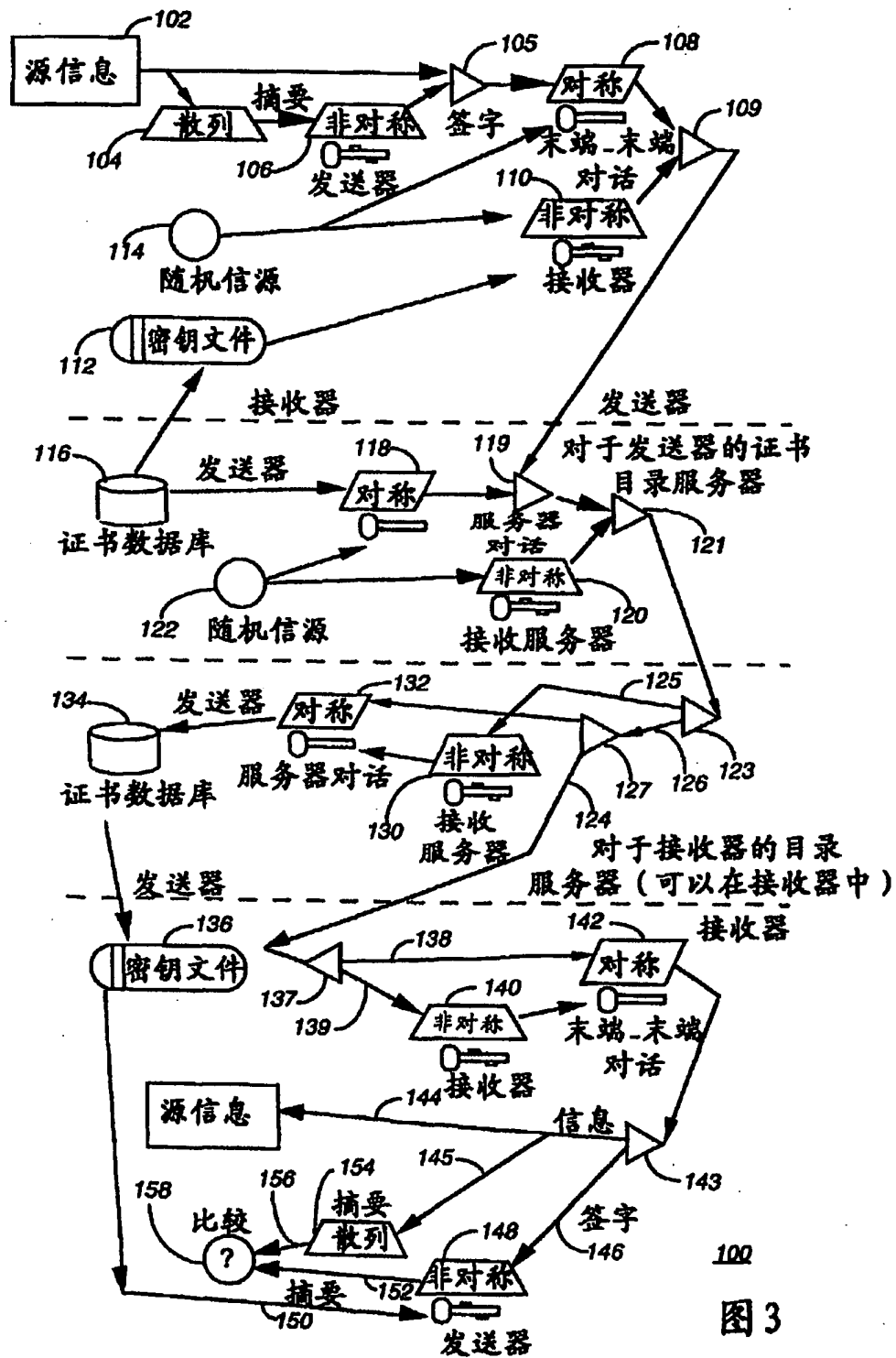


图 3

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.